* Multiple encryption is a technique in which an encryption algorithm is used multiple times.

- In first instance plaintext is converted into cipher text using the encryption algorithm. This ciphertext is then used as input & the algorithm is applied again. This process may be repeated through any number of stages.

* A mode of operation is a technique for enhancing the effect of cryptographic algorithm or adapting the algorithm for an application, such as applying a block cipher to a sequence of data blocks or a data stream.

- Five mode of operation for use with symmetric block ciphers such as DES & AES
  - Electronic codebook mode
  - cipher block chaining mode
  - cipher feedback mode
  - output feedback mode
  - counter mode.

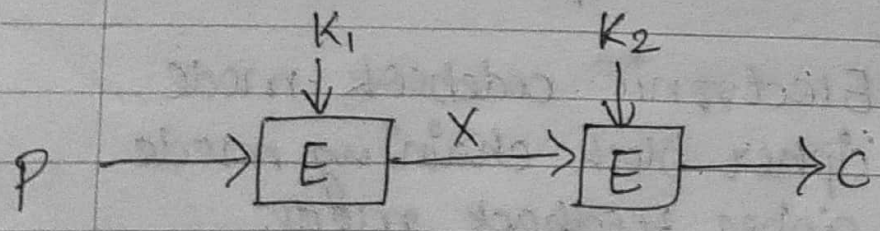
To overcome the vulnerabilities of DES to a bruteforce attack, many alternatives are there.

1. AES Algo
2. use multiple encryption with DES & multiple keys. (double DES, 3-DES).

* Double DES.

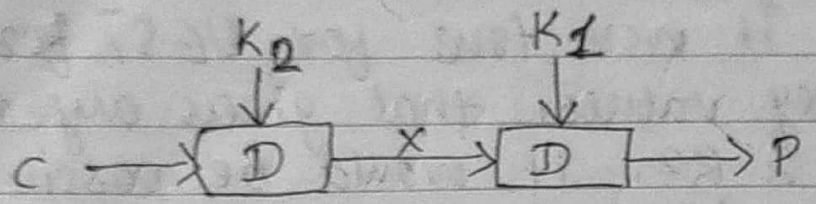
The simplest form of multiple encryption has two encryption stages & two keys.

Given plaintext P & encryption key K_1 & K_2, ciphertext C is generated as below:



Encryption $C = E(K_2, E(K_1, P))$

Decryption requires that the keys be applied in reverse order:



Decryption

$$P = D(K_1, D(K_2, C))$$

- here key length = 56 x 2 = 112 bits

resulting in dramatic increase in cryptographic strength.

for Brute force attack = 2^{112} possibilities

[∵ key length = 112 bits
K_1 = 56 bits
K_2 = 56 bits]

Adv: Stronger than DES

Drawbacks.

(1) Reduction to single stage.

Suppose it were true for DES, for all 56-bit key values, that given any two keys K1 & K2, it would be possible to find a key K3 such that

$$E(K_2, E(K_1, P)) = E(K_3, P)$$

If it is the case the double encryption & indeed any number of stages of multiple encryption with DES,

would be useless because the result would be equivalent to a single encryption with a single 56-bit key.

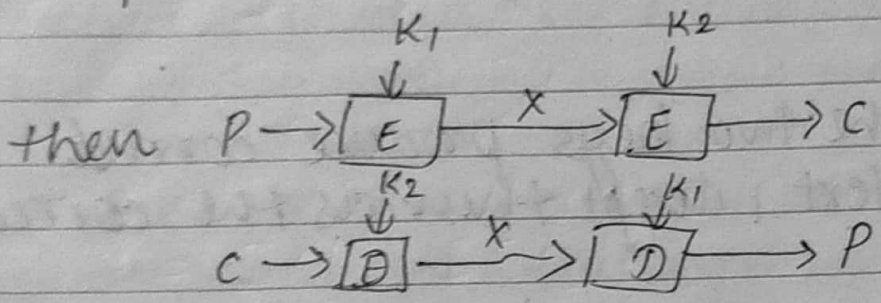
(2) Meet-in middle Attack

[it does not depend on any particular property of DES but that will work against any block encryption cipher]

If we are having.

$$C = E(K_2, E(K_1, P))$$

$$P = D(K_1, D(K_2, C))$$



$$\text{so} \quad X = D(K_2, C) = E(K_1, P)$$

Given known pair (P, C), the attack can be proceed as follow.

① encrypt P for all 2^{56} possible value of K_1

[get X for all possible 2^{56} value of K_1]

② Decrypt C using all 2^{56} possible value of K_2.

[get another 2^{56} possible values of X with K_2]

Then match all possibilities of X.

If any match found, test two keys against known plaintext - ciphertext pair

If the two keys produce correct ciphertext, accept them as the correct key.

* Block cipher modes of operation

A mode of operation is a technique for enhancing the effect of cryptographic algorithm or adapting the algorithm for an application, such as applying a block cipher to a sequence of data blocks or a datastream.

1. Electronic codebook mode
2. Cipher block chaining.
3. Cipher feedback
4. Output feedback
5. Counter.

1. Electronic codebook mode:-

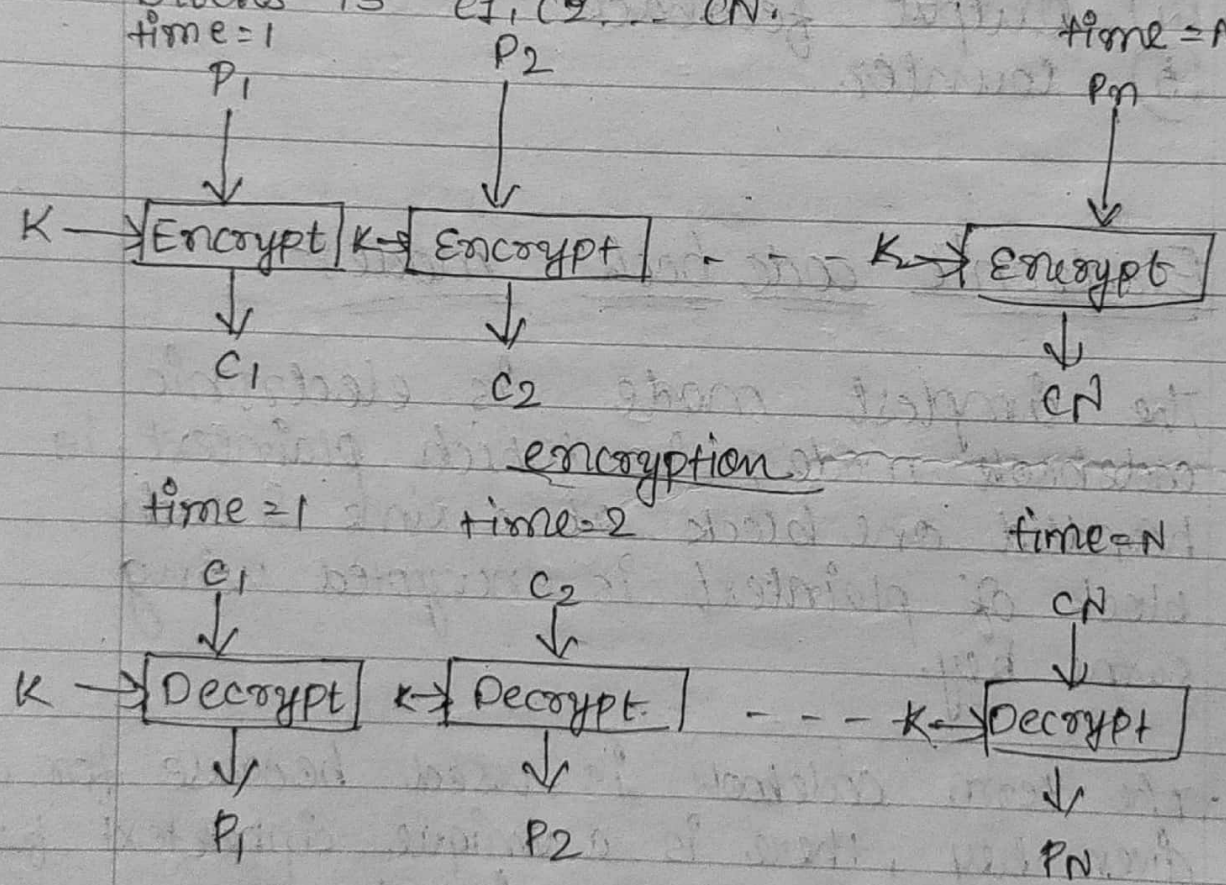
The simplest mode is electronic codebook mode, in which plaintext is handled one block at a time & each block of plaintext is encrypted using same key.

The term codebook is used because for a given key, there is a unique ciphertext for every b-bit block of plaintext.

For a message longer than b-bits, the procedure is simply to break the message into b-bit blocks, padding the last block if necessary.

Decryption is performed on block at a time, always using same key.

In below figure, the plaintext consists of sequence of b-bit blocks, $P_1, P_2, \ldots P_N$; the corresponding sequence of ciphertext blocks is $C_1, C_2 \ldots C_N$.



encryption

Decryption

The ECB method is ideal about a short amount of data, such as an encryption key.
Thus if you want to transmit a DES key securely, ECB is appropriate mode to use.

Disadvantage / Drawback

The most significant characteristic of ECB is that the same 64-bit block of plaintext, if it appears more than once in the message, always produces the same ciphertext.

For lengthy msgs, the ECB may not be secure. If the msg is highly structured, it may be possible for a cryptanalyst to exploit this regularity.

Q] Cipher Block chaining mode. (CBC)

To overcome security deficiencies of ECB we would like there is a technique in which the same plaintext block, if repeated, produces different ciphertext blocks which is ~~known as~~ as chipher block chaining mode.

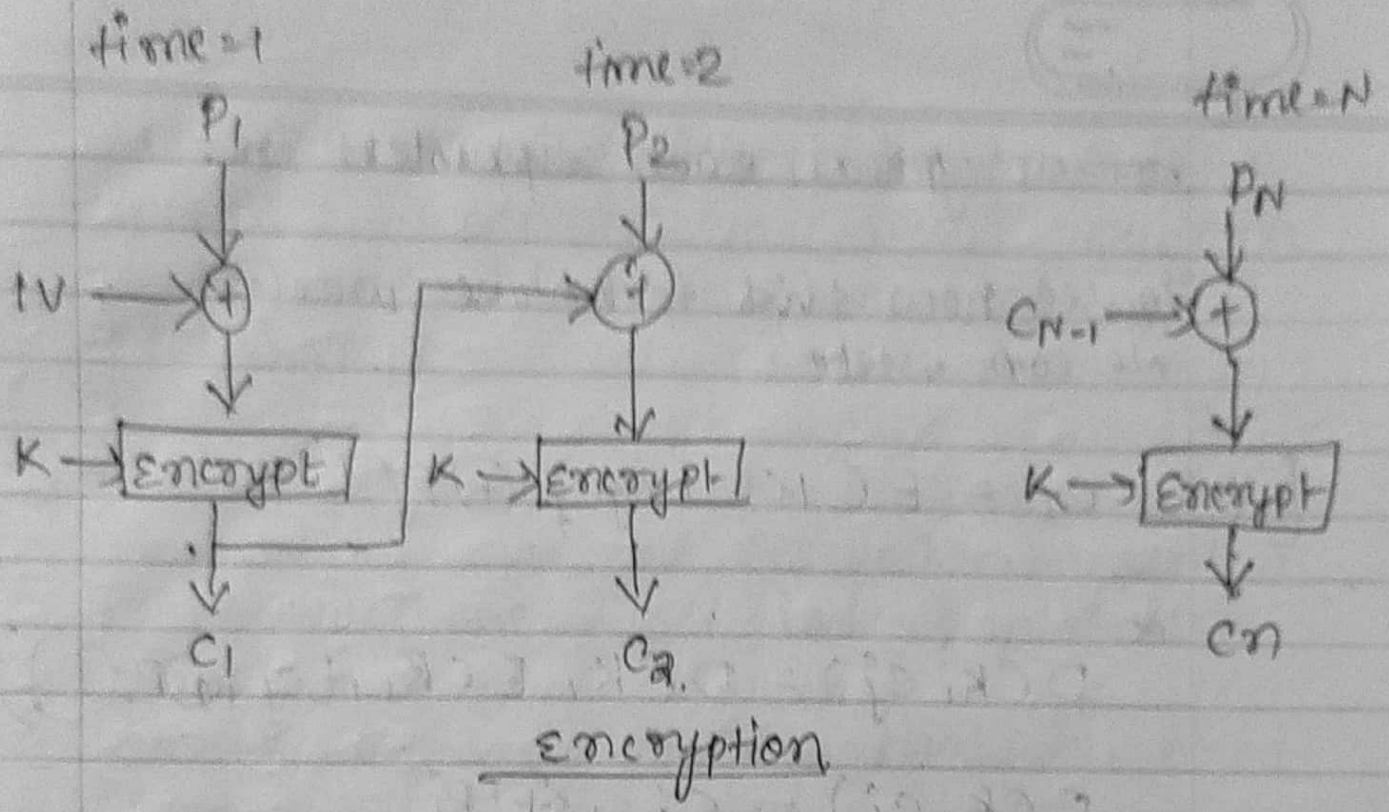
In this scheme, the input to the encryption algorithm is the XOR of the current plaintext block & the preceeding ciphertext block.

The same key is used for each block.

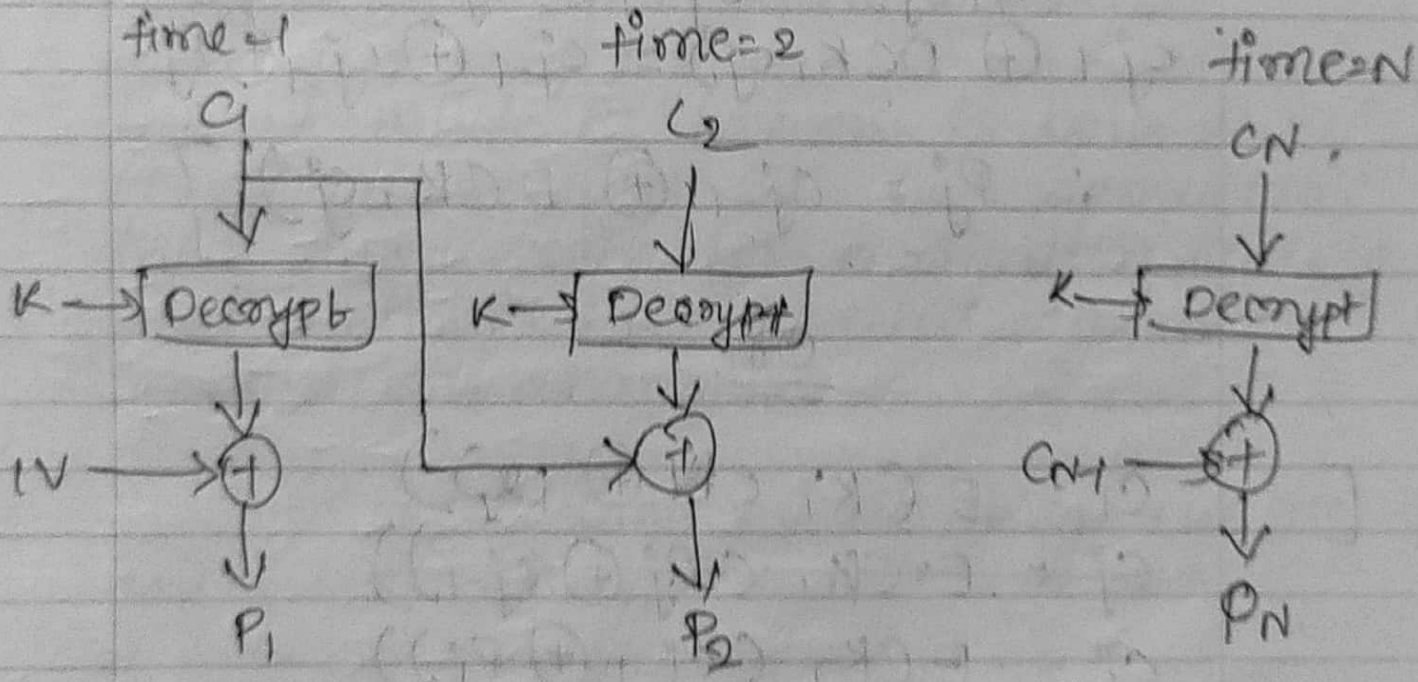
In effect, the input to the encryption function for each plaintext block bears no fixed relationship to the plaintext block. Therefore, repeating patterns of bits are not exposed.

For decryption each cipher block is passed through the decryption algorithm. The result is XORed with the preceding ciphertext block to produce the plaintext block.

W.



Encryption



Decryption

For decryption, each ciphertext blo

To see how this technique works, we can write

$$C_1 = E(K, [C_{j-1} \oplus P_j])$$

&

$$D(K, C_j) = D(K, E(K, [C_{j-1} \oplus P_j]))$$

$$D(K, C_j) = C_{j-1} \oplus P_j$$

$$C_{j-1} \oplus D(K, C_j) = C_{j-1} \oplus C_{j-1} \oplus P_j$$

$$\therefore P_j = C_{j-1} \oplus D(K, C_j)$$

or

$$C_1 = E(K, (IV \oplus P_1))$$

~~$C_j = E(K, (P_j \oplus C_{j-1}))$~~

$$C_j = E(K, (C_{j-1} \oplus P_j))$$

$$P_1 = IV \oplus D(K, C_1)$$

$$P_j = C_{j-1} \oplus D(K, C_j)$$

IV → Initialization vector

Here, to produce the first block of ciphertext, an Initialization vector (IV) is XORed with the first block of plaintext.

On decryption the IV is XORed with the output of the decryption algorithm to recover the first block of plaintext.

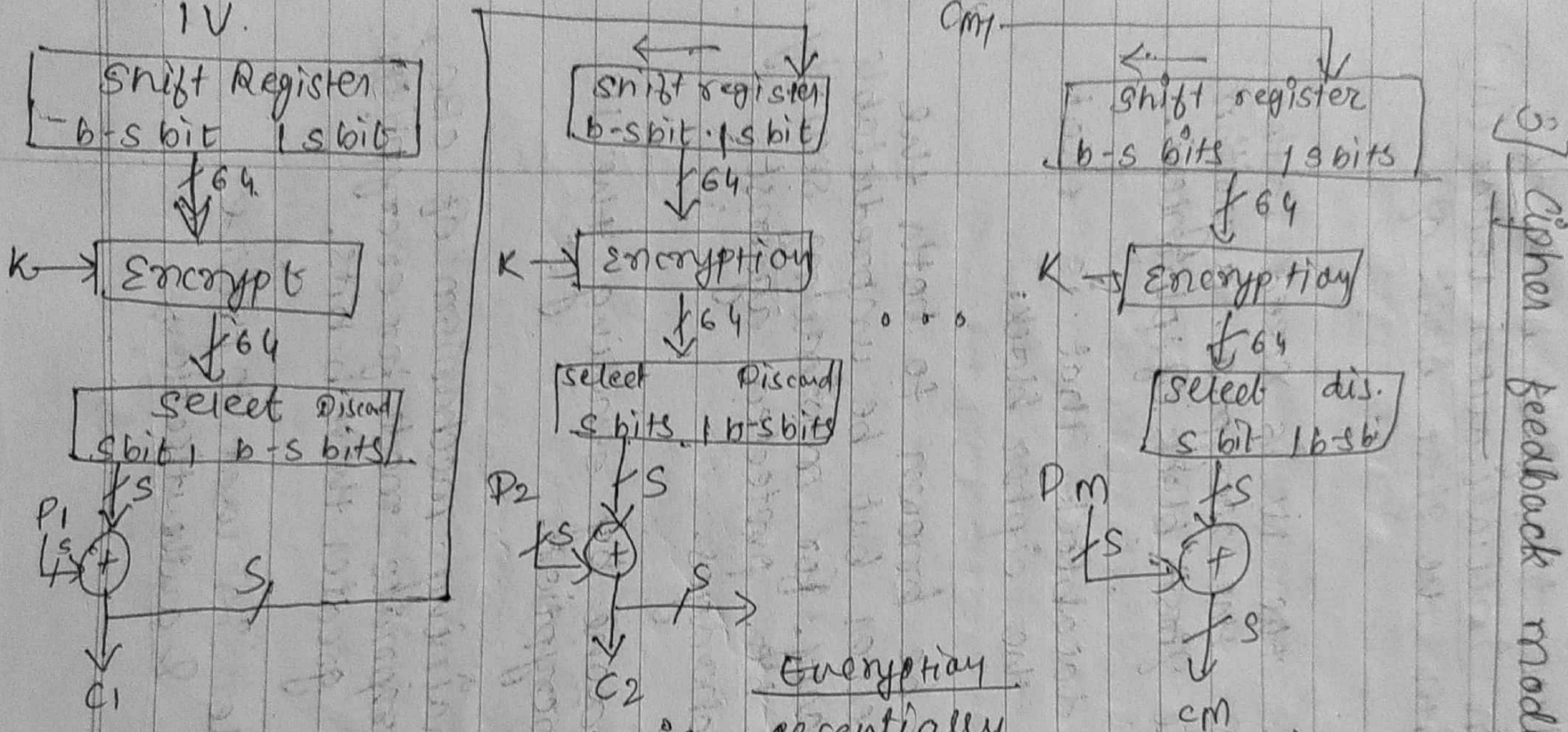
The IV is a datablock that is that same size as the cipher block.

The IV must be known to both the sender & receiver but be unpredictable by a third party. For maximum security, the IV should be protected against unauthorized changes.

This could be done by sending the IV using ECB encryption.

- Because of chaining mechanism of CBC, it is an appropriate mode for encrypting msgs of length greater than b-bits.

The CBC mode is used to provide confidentiality & authentication.



- The DES scheme is essentially a block cipher technique that uses b bit blocks. However, it is possible to convert DES into stream cipher using either the CFB or Output feed mode

[Draw fig. of decry. as same as encryption just replace place of P_i & C_i]

3) Cipher feedback mode (

Fig. depicts the CFC scheme. On the figure, it is assumed that the unit of transmission is s bits;
a common value of s is s=8.

As with CBC, the unit of plaintext are chained together, so that the ciphertext of any plaintext unit is function of all the preceding plaintext. but in this case rather than units of b bits, the plaintext is divided into segments of s bits.

On encryption,

- input to the encryption function is a b-bit shift register that is initially set to some initialization vector.

- The leftmost s bits of the output of the encryption is XORed with the first (s bits) segment of plaintext P_1 to produce first unit of ciphertext C_1. which is then transmitted.

here contents of the shift register are shifted left by s-bits & C_1 is placed in right most sbits of the shift register. This process continues

fig - 8 decoy will be same rather than place of C_1 & P_1.

until all plaintext units have been encrypted.

- In decryption,

the same scheme will be used, except that the received ciphertext unit is XORed with the output of the encryption function to produce the plaintext unit.

Here for decryption encryption fun. is used,

$$C_1 = P_1 \oplus S_s(E(K, IV))$$

$S_s(x)$ most significant s bits of x.

drawback:- [If there is an error in transmission ~~encryption~~ process in 1st character or 1 bit of 1st block then error will propogate in next round.

So whole o/p will be wrong.]

[bit error propogation]

ex: if error in C_1 then it will effect C_2, C_3 -- also.

4] Output feedback mode.

The output feedback mode is similar in structure to CFB. as show in fig.

- As we can see, it is output of the encryption function that is fed back to the shift register in OFB, whereas in CFB the cipher text unit is fed back to the shift register.

Ad. bit error in transmission don't propogate.

dis. more vulnerable to a msg modification attack than in CFB.

5] Counter mode:- (CTR)

counter mode is used with ATM, network security & IPSec.

fig...

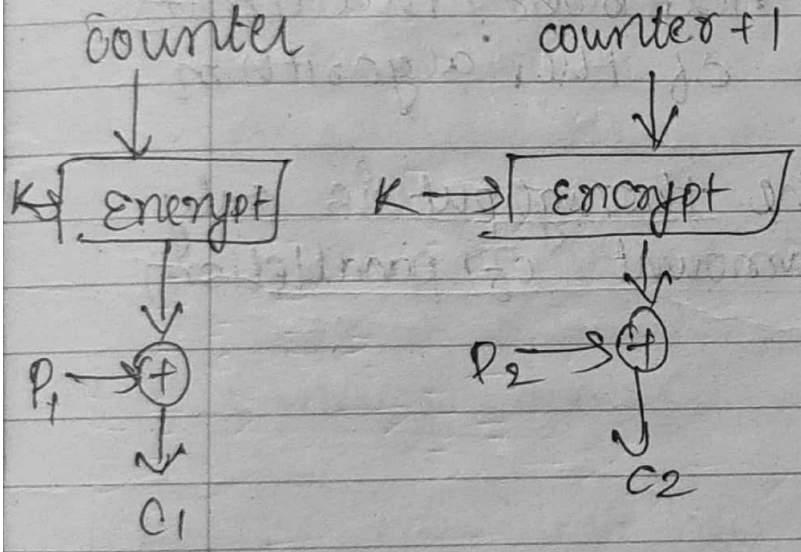
A counter, equal to plaintext block size is used & the counter value must be different for each plaintext block that is encrypted.

Typically counter is initialized to some value & then incremented by 1

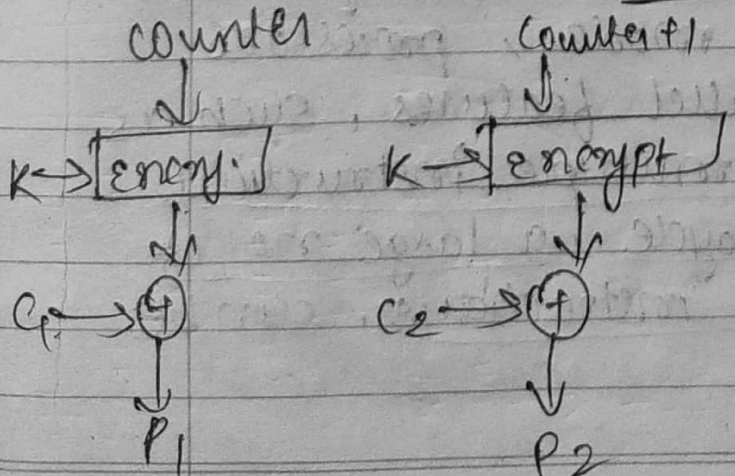
for each subsequent block.

For encryption, the counter is encrypted & then XORed with the plaintext block to produce the ciphertext block; there is no chaining.

For decryption, the same sequence of counter value is used with each encryption counter, XORed with a ciphertext block to recover the corresponding plaintext block.



Encryption



Advantages.

* Hardware efficiency:-

Unlike in three chaining modes, encryption in CTR can be done in parallel on multiple blocks of plaintext or ciphertext

while in chaining mode, computation must be completed on one block before beggining on the next block. This limits max. throughput of the algorithm

On CTR mode the throughput is only limited by the amount of parallelism that is achieved.

* Software efficiency:

Because of opportunities for parallel execution in CTR mode, processors that support parallel features, such as aggressive pipeling, multiple instruction dispatch per clock cycle, a large no. of register & SIMD instructions, can be effectively utilized.

* Preprocessing:-

The execution of the underlying encryption algorithm doesn't depend on input of the plaintext or ciphertext.

Therefore if sufficient memory is available & security is maintained, preprocessing can be used to prepare the o/p of the encryption boxes that feed into XOR functions.

When ciphertext or plaintext input is presented, then the only computation is a series of XORs, such a strategy greatly enhances throughput

* Random Access

The ith block of plaintext or ciphertext can be processed in random fashion

There may be application in which all ciphertext are stored, & it is desired to decrypt just one block, for such applications the random access fashion is attractive.

* Provable security.

as secure as other modes.

* Simplicity.

CTR required only implementation of encryption algorithm & not the decryption algorithm.

[So here decryption key scheduling need not be implemented]